



**SASKATCHEWAN INFORMATION
AND PRIVACY COMMISSIONER**

2008 - 2009 ANNUAL REPORT

"The modern totalitarian state relies on secrecy for the regime, but high surveillance and disclosure for all other groups."

"The democratic society relies on publicity as a control over government, and on privacy as a shield for group and individual life"

Alan F. Westin

2008 - 2009 ANNUAL REPORT

Saskatchewan
Information and Privacy
Commissioner



503 - 1801 Hamilton Street
Regina, Saskatchewan
S4P 4B4

Tel: (306) 787-8350
Fax: (306) 798-1603
Website: www.oipc.sk.ca

June 29, 2009

Hon. D. Toth
Speaker of the Legislative Assembly
129 Legislative Building
Regina, Saskatchewan
S4S 0B3

Dear Mr. Speaker:

I have the honour to present to the Legislative Assembly my 2008-2009 Annual Report in accordance with the provisions of section 62(1) of *The Freedom of Information and Protection of Privacy Act*, section 52(1) of *The Local Authority Freedom of Information and Protection of Privacy Act* and section 60(1) of *The Health Information Protection Act*.

Respectfully submitted,

A handwritten signature in black ink, appearing to read 'R. Gray Dickson', written over a circular stamp or seal.

R. Gray Dickson, Q.C.
Saskatchewan Information and Privacy Commissioner
Encl.

Table of Contents

Introduction	Page 1
Mandate of the Commissioner.....	Page 2
Mission Statement.....	Page 2
Commissioner's Message.....	Page 3
Organization Chart	Page 10
<i>The Freedom of Information and Protection of Privacy Act (FOIP)</i>	Page 11
PROGRESS HAS BEEN MADE	Page 11
MORE NEEDS TO BE DONE	Page 11
Private Sector Workers Should Not Go Unprotected	Page 12
Approach of The Workers' Compensation Board (WCB)	Page 14
Why Should Municipal Police Services Not Be Subject to <i>The Local Authority Freedom of Information and Protection of Privacy Act?</i>	Page 15
ADVICE AND COMMENTARY	Page 16
Enhanced Driver's License	Page 16
Administrative Tribunals and the Internet	Page 20
Privacy Impact Assessment for Saskatchewan Laboratory Results Repository (SLRR)	Page 21
TOOLS AND PUBLICATIONS	Page 22
RIGHT TO KNOW	Page 23
<i>The Local Authority Freedom of Information and Protection of Privacy Act (LA FOIP)</i>	Page 25

Table of Contents

<i>The Health Information Protection Act (HIPA)</i>	Page 26
ACCOUNTABILITY	Page 28
COMPULSORY (NON-CONSENTED) UPLOADING	Page 28
SECONDARY USES AND DISCLOSURES	Page 29
TOO MANY PRIVACY BREACHES	Page 30
PRAIRIE HEALTH INFORMATION DAY	Page 30
Use of Privacy Impact Assessments	Page 31
National meeting of Oversight Agencies held in Saskatchewan	Page 32
Growing Public Awareness	Page 34
Capacity of the OIPC	Page 35
How to Make an Access Request	Page 36
How to Make a Privacy Complaint	Page 37
Case Summaries	Page 39
Budget Plan, Budget & Statistics	Page 41
Measuring Up	Page 42
Performance Measures for 2008 - 2009	Page 42
Statistical Review of 2008 - 2009	Page 49
Financial Statements	Page 54
Appendix I - Definitions	Page 68
Appendix II - Sample List of Presentations	Page 72
Appendix III - List of Bodies Subject to OIPC Oversight	Page 73
Endnotes	Page 76

Introduction

The role of the Information and Privacy Commissioner has sometimes been described as that of the umpire in the information age.

That role has also been described as follows:

Our recent comparative analysis of privacy protection policy has concluded that, regardless of legislative powers, every data-protection commissioner in Canada and elsewhere is expected at some point to perform seven interrelated roles: ombudsman, auditor, consultant, educator, policy adviser, negotiator, and enforcer.¹

In 1992, *The Freedom of Information and Protection of Privacy Act* (FOIP) was proclaimed. This enshrined two principles:

1. public records must be accessible to the public; and
2. "personal information" must be protected by public bodies.

FOIP applies to all "government institutions". This captures all Ministries of the Saskatchewan Government plus Crown corporations, Boards, Commissions and Agencies.

In 1993, *The Local Authority Freedom of Information and Protection of Privacy Act* (LA FOIP) was proclaimed. This law is very similar to FOIP, but applies to "local authorities" such as schools, universities, regional health authorities, municipalities, and library boards.

In 2003, *The Health Information Protection Act* (HIPA) was proclaimed. This applies to organizations and individuals designated as a health information "trustee", defines the rules for what is "personal health information" and how that personal health information can be collected, used and disclosed. It also provides a right of access to personal health information and a right to seek correction of errors.

The Supreme Court of Canada has declared that laws like FOIP, LA FOIP and HIPA are special kinds of laws that define fundamental democratic rights of citizens.² They are "quasi-constitutional" laws that generally are paramount to other laws.



Mandate of the Commissioner

There are four major elements in the Saskatchewan Information and Privacy Commissioner's (Commissioner) mandate defined by FOIP, LA FOIP and HIPA:

- 1** The Commissioner responds to requests for review of decisions made by government institutions, local authorities or health information trustees in response to access requests, and makes recommendations to those bodies.
- 2** The Commissioner responds to complaints from individuals who believe their privacy has not been respected by government institutions, local authorities or health information trustees, and makes recommendations to those bodies.
- 3** The Commissioner provides advice to government institutions, local authorities or health information trustees on legislation, policies or practices that may impact citizens' access or privacy rights.
- 4** The Commissioner provides education with respect to information rights including both access to information and protection of privacy.

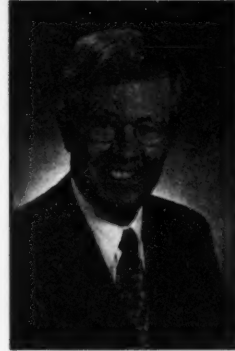
Mission Statement

**The people of Saskatchewan shall enjoy the full measure of
information rights that have been affirmed by the
Legislative Assembly of Saskatchewan**



Commissioner's Message

The year 2008-2009 could be described as
the year of the privacy breach in Saskatchewan.



Four years ago we had only two privacy investigations. In 2008-2009 we opened 62 new privacy investigations. This includes:

- multiple investigations (14) into abandoned patient files;
- a municipality sending information including social insurance numbers, health and pension information on 2000 employees and citizens to a researcher in error;
- personal health information found on used fax equipment sold as surplus;
- unsecured personnel and inmate records at a correctional centre;
- inappropriate sharing of personal health information by health professionals;
- posting full text administrative tribunal decisions on the Internet without masking personal identifiers;
- an employer shared psychological assessment with too many people who had no need to know;
- employment and financial information provided to the wrong person;
- a flash drive containing personal health information stolen;
- the wrong wristband put on patient in acute care facility;
- personal health information of patient available through link on Internet; and
- personal health information sent to the wrong people via mail and fax.

These investigations have occurred under each of the three laws that we oversee, FOIP, LA FOIP and HIPA, and in every corner of our province.



Commissioner's Message

I view these cases as serious and troubling. Such cases or at least the facts giving rise to these investigations tend to undermine public confidence in our public institutions and our health information trustees.

This has serious consequences for the ability of our public institutions to move from paper systems to digital information systems and to deliver high-quality service to Saskatchewan residents. Such a transformation requires public support to be successful and to ensure that the benefits of digital information systems can be maximized.

The reasons for breaches identified in investigations our office has undertaken are varied. Some common reasons include:

- Lack of privacy leadership within an organization,
- Absence or inadequate privacy policy, and
- Absence or inadequate privacy training.

In most cases, we have found that the leadership of the public body or the trustee is embarrassed by the breach, recognizes that it must do better and is open to our suggestions for remedial action to minimize a reoccurrence.

This explosion in the volume of breach of privacy complaints, however, constitutes the single most significant change in our caseload since the appointment of a full-time Information and Privacy Commissioner in 2003.



Commissioner's Message

My concern with the increase in both the volume and gravity of privacy breaches needs to be tempered by two important qualifications:

1

The Office of the Information and Privacy Commissioner (OIPC) oversees at least 3000 organizations. With only four investigators we cannot begin to audit the safeguards taken or neglected by all of those organizations. Consequently, it may be dangerous to extrapolate from the breaches that come to our attention and paint all public institutions with the same brush. The fact that we have not yet received notice of more privacy breaches may reflect the implementation of good privacy practices and appropriate controls in many of those institutions. Our direct experience however suggests that there may be more problems that, for a variety of reasons, have not yet come to our attention.

2

The other qualification is that readers may be surprised to learn that many, if not most, of the complaints that come to our attention are self-reported by the government institution or local authority or health information trustee. I view this as a positive development. It reflects an appropriate awareness of the seriousness of privacy breaches and a realization that those bodies need to do a better job of protecting privacy. I have been encouraged by the willingness of the bodies we oversee to self-report to our office. I want to work hard to encourage the continuation of that kind of collaboration.

What lessons can be learned from our experience with data breaches?



Commissioner's Message

(a) Leadership

Trustees, government institutions and local authorities require two kinds of leadership:

1 The Deputy Minister or Chief Executive Officer of the organization doesn't need to be familiar with all of the nuances of privacy legislation and best practices. That leader does, however, need to understand that the requirements of the applicable legislation are of high importance. The leader needs to signal to the men and women in that organization that protecting the privacy of those citizens that it deals with is a priority.

2 Each organization should appoint and then adequately resource a FOIP Coordinator position. In the case of health information trustees this would be a HIPA Coordinator or Privacy Officer. The position of FOIP Coordinator should be sufficiently senior to the point that the FOIP Coordinator will have ready access to the Deputy Minister or CEO to provide largely unfiltered advice on privacy and access compliance. Except for larger organizations, this designation would likely be assigned to an individual that also has other job responsibilities.

(b) Access and Privacy Policy and Procedures

Privacy policy needs to be clear, unambiguous and accessible to all public sector and trustee employees. A surprising number of the organizations we oversee have no privacy policy or have one that is wholly inadequate for its compliance needs. High level policies that offer vague generalities are practically useless. The need is for concrete, practical policy that addresses the typical issues and problems that confront public bodies and trustees on a day-to-day basis. The policy and procedures need to address administrative, physical and technological safeguards.



Commissioner's Message

(b) Access and Privacy Policy and Procedures (cont'd)

We have encouraged the Access and Privacy Branch, Ministry of Justice and Attorney General (the Branch) to provide government institutions and local authorities with templates and sample policies to assist them in their compliance efforts. To the same end, we have encouraged Saskatchewan Health and the health profession regulatory bodies to provide health trustees with similar materials to assist in HIPA compliance efforts.

I recognize that both Saskatchewan Justice and Saskatchewan Health have made good progress over the last year in providing support to the public bodies and trustees subject to FOIP and LA FOIP and HIPA. This work needs to be ongoing as we accumulate more experience with the application of these laws. Our office appreciates the collaborative approach that both the Branch in Saskatchewan Justice and the Access and Privacy team at Saskatchewan Health have taken with our office. We also value the regular meetings between our respective offices.

There continues to be a need for more work to be done by the health profession regulatory bodies to assist their members in terms of HIPA compliance. In our experience simply too many health professionals are not compliant with HIPA, particularly section 16 and the requirement to have policies and procedures for administrative, technical and physical safeguards.

(c) Access and Privacy Training

There is certainly far more training available now than would have been the case just five years ago. The website for the Branch now provides a wealth of material for both government institutions and local authorities including an online training course that seems to be heavily used by those public bodies. The Branch has also published a series of information sheets, checklists, model letters and reference to many useful resources and tools. I encourage all government institutions and local authorities to become familiar with these resources and to make better use of them. The most significant gap in the materials offered by the Branch is detailed information on the application of mandatory and discretionary exemptions. I am encouraged that the Branch acknowledges that need and is attempting to address it, resources permitting.



Commissioner's Message

(c) Access and Privacy Training (cont'd)

In Saskatchewan many non-profit agencies contract with government institutions, local authorities and trustees to provide services for defined fees. In some cases this entails a good deal of personal information or personal health information being supplied to or accumulated by the agency for purposes of that contract. In our experience, many of those contracting agencies have weak or non-existent privacy policies or procedures.

Several years ago we produced the booklet, *The Contractors Guide to Access and Privacy in Saskatchewan* which is available on our website for downloading. Given the lack of administrative staff and budget common to many of these agencies, I recommend that those government institutions, local authorities and trustees engaged in these fee for service arrangements offer FOIP workshops and training sessions specifically for staff of the agencies.

THE GAPING HOLE PERSISTS

To borrow from the *Privacy and Access: A Saskatchewan Roadmap for Action* in our 2004 - 2005 Annual Report³ ("Roadmap for Action") the campaign to communicate the importance of privacy protection is undercut by what I have described as a 'gaping hole' in our FOIP and LA FOIP Acts. This gaping hole is the absence of a provision that requires a public body to take reasonable steps to safeguard personal information (including personal health information).

As previously recommended to the Legislative Assembly (Assembly), such a provision should be supported or reinforced by an offence and a substantial penalty. This would be in order of the \$50,000 maximum fine under HIPA for an individual and the \$500,000 maximum fine for an organization. The current maximum penalty in FOIP is only \$1,000 and that is restricted to interference with our office in its work.⁴

A similar gaping hole exists in the federal *Privacy Act*. I note though that the House of Commons Standing Committee on Access to Information, Privacy and Ethics has been hearing submissions on addressing that deficiency from groups including the Canadian Bar Association.⁵



Commissioner's Message

CONCLUSION

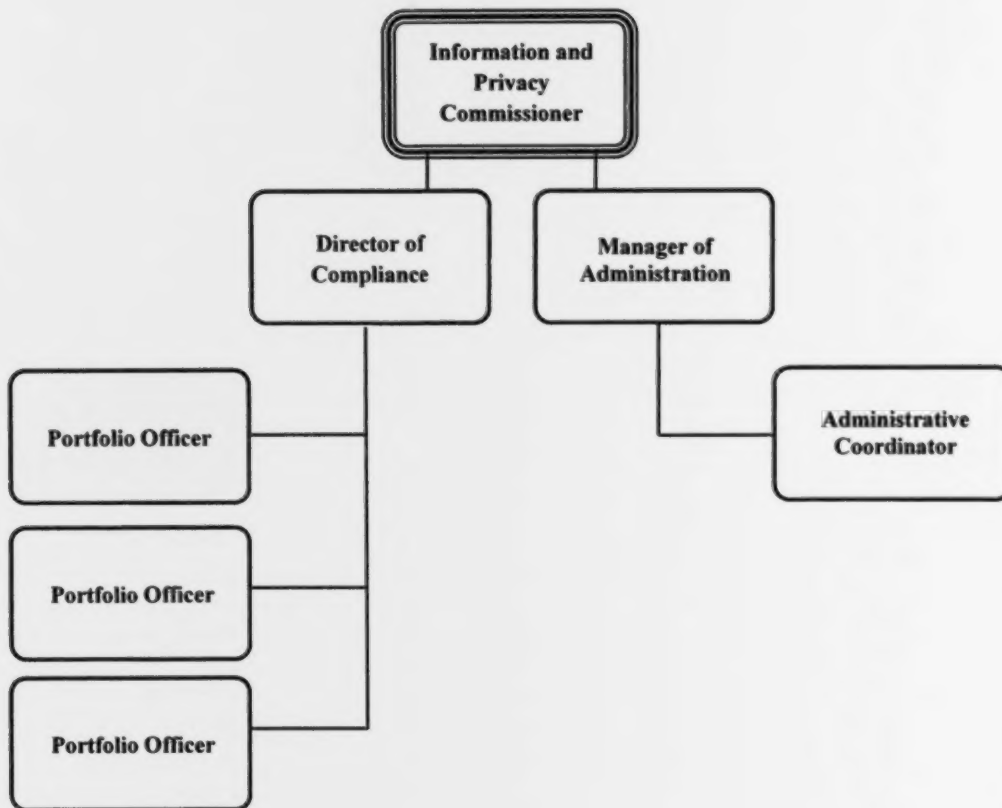
I am grateful for the support I have received from and for the excellent work done by the dedicated staff in our office. As in past years, I wish to acknowledge the assistance provided to me and to our office by the Legislative Assembly Service including its Human Resource and Payroll Services, Financial and Administrative Services and Communication and Technology Services branches.

Near the end of the 2008 - 2009 fiscal year the Assembly reappointed me for a further five-year term. I value the confidence that the Members have demonstrated by virtue of the reappointment. I am looking forward to further progress in all facets of our broad statutory mandate.

Gary Dickson, Q.C.
Saskatchewan Information and Privacy Commissioner



Organization Chart



The Freedom of Information and Protection of Privacy Act (FOIP)

I am encouraged that the Saskatchewan Government has repeatedly and publicly stressed the need to be transparent and accountable. I note that in past Annual Reports of this office, I have prescribed a number of concrete steps that could be taken to further that goal of higher transparency and accountability to the residents of Saskatchewan. This includes *Roadmap for Action* in my 2004-2005 Annual Report.⁶ I continue to encourage the Government and the Assembly to deal with those outstanding recommendations without further delay.

PROGRESS HAS BEEN MADE

As already noted, there has certainly been steady progress in enhancing awareness of government institutions and local authorities about their obligations under FOIP and LA FOIP respectively. In this regard, I want to acknowledge the continued efforts of the Branch. In my experience the need for assistance far outstrips the capacity of that Branch to assist. To expect that an office of three persons can adequately address the needs of many thousands of public sector workers is just unrealistic.

As noted in earlier Annual Reports, we must be mindful that our legislation is 17 years old and that as a result of neglect and indifference for at least the first 11 years, there is a remarkable pent-up demand for assistance now. I encourage the Minister of Justice and Executive Council to consider increasing the size and capacity of this important branch.

MORE NEEDS TO BE DONE

Although I repeat and incorporate by reference in this Annual Report all of the recommendations from the Saskatchewan *Roadmap for Action*, I want to emphasize a couple of recommendations that are particularly urgent.



The Freedom of Information and Protection of Privacy Act (FOIP)

Private Sector Workers Should Not Go Unprotected

We continue to receive many calls from employees of the private sector who wish to have breach of privacy complaints investigated. These callers are both surprised and distressed when we advise them that unlike employees in British Columbia and Alberta they are essentially unprotected when it comes to abuse of their information privacy rights. They are confused that there is completely unequal treatment of employees depending on whether they work for a private sector employer or a public sector employer.

The employee in Saskatchewan's public sector has the full range of protection guaranteed by Part IV of the FOIP and LA FOIP Acts. This includes the right to have our oversight office investigate their complaints, at no direct cost to the complainant. Contrast that with the employee in the private sector whose only recourse is to hire a lawyer and start a lawsuit under the little used Saskatchewan *Privacy Act*⁷ for damages resulting from a willful breach of privacy. There may be limited protection to a private sector employee subject to a collective agreement that addresses information privacy.

The costs of hiring counsel and the courts historic reluctance to provide meaningful compensation in breach of privacy cases effectively deters many employees from taking any action. This differential treatment is hard to justify since an employer will usually have much more extensive and prejudicial information about its employees than it will have about its customers. The employer will often have relationship information, health information, financial information, work evaluation information and increasingly, biometric information about its employees.



The Freedom of Information and Protection of Privacy Act (FOIP)

Private Sector Workers Should Not Go Unprotected (cont'd)

I respectfully submit that in 2009 it is unacceptable that this sensitive personal information is at risk simply because one chooses to work in the private sector rather than the public sector. It would be hard to imagine a human rights code, employment standards or occupational safety rules that applied only to the public sector and completely exempted the private sector. Nonetheless, that is precisely the situation we currently have in our province when it comes to the protection of employee privacy. I should note that those employees who work for an enterprise that qualifies as a 'federal work, undertaking or business' such as airlines, banking, telecommunications and inter-provincial trucking are covered by *Personal Information Protection of Electronics Document Act* (PIPEDA).¹⁰ This likely would mean protection for a very small portion of Saskatchewan's private sector workforce.

There are two further issues addressed in previous Annual Reports that warrant highlighting in this report. These are two significant gaps in terms of FOIP coverage. One is the approach taken by the Saskatchewan Workers' Compensation Board (WCB) and the other is the apparent exclusion of municipal police services from the scope of FOIP.



The Freedom of Information and Protection of Privacy Act (FOIP)

Approach of The Workers' Compensation Board (WCB)

In virtually all other Canadian jurisdictions, WCB is subject to access to information legislation just like every other public body in those jurisdictions. In Saskatchewan however, the WCB has taken an interesting and, in our view, legally unfounded interpretation of section 171.1 of its enabling legislation to deny applicants access to their own personal information.¹¹ Unfortunately, our office has no jurisdiction to put this before a court to have the question of interpretation resolved once and for all. In the result, there is a kind of stalemate, with WCB denying access requests routinely unless an appeal has been launched by the worker and the appeal is deemed proper and appropriate.

I should note that we raised this question before the last Saskatchewan Workers' Compensation Act - Committee of Review and that Committee in its final report endorsed our position.¹² I am therefore urging the Saskatchewan Government to ensure that this long standing recommendation from our office, as endorsed by the Committee of Review, be implemented.

The WCB continues to assert that it need not comply, as every other government institution does, with the 'access to information' obligations of the FOIP Act. This is very strange and, in my view, indefensible. I am not aware of any other Canadian jurisdiction that views its WCB apparatus as so vulnerable and overwhelmed that it must be carved out of FOIP and be able to frustrate the legitimate requests of thousands of workers to access their own personal health information and personal information that is in the possession or control of WCB.

What is surprising is that the action of WCB in limiting access to cases where an appeal has been initiated had been brought to the Assembly's attention as early as 1981. That was the year that former Chief Justice E.M. Culliton submitted his extensive report - *On The Matter of Freedom of Information and Protection of Privacy in the Province of Saskatchewan*. Culliton questioned why the requirement for disclosure should arise only in the event of an appeal.¹³



The Freedom of Information and Protection of Privacy Act (FOIP)

Why Should Municipal Police Services Not Be Subject to *The Local Authority Freedom of Information and Protection of Privacy Act*?

The experience over the last 26 years with public sector access and privacy legislation in Canadian jurisdictions confirms that police services tend to receive a large percentage of access to information requests and privacy complaints. This reflects the large volume of personal information that police services collect, use and disclose in the course of their important work. This also reflects the view in most Canadian jurisdictions - ensuring police services are subject to laws like FOIP is an important feature in ensuring that police services meet high standards of accountability and transparency to ensure high levels of public trust.

To my knowledge, municipal police services are subject to freedom of information and protection of privacy laws in every other jurisdiction in Canada with the exception of Prince Edward Island and Saskatchewan. I have raised this several times with the former Government and renew this recommendation with the current Government. The fact that Saskatchewan has legislation creating the Public Complaints Commission in no way obviates the need to oversee the access to information and privacy activities of municipal police services.

Oddly, the existing situation means we have in Saskatchewan a two-tiered system of accountability and transparency when it comes to police services. If you live in a community where the Royal Canadian Mounted Police provide municipal policing, you have the protection and access rights afforded under the federal *Access to Information Act*.¹⁴ You would also have the protection and privacy rights afforded under the federal *Privacy Act*.¹⁵ No equivalent protection is afforded Saskatchewan residents who live in communities served by their own municipal police service.



The Freedom of Information and Protection of Privacy Act (FOIP)

ADVICE AND COMMENTARY

Our office continues to be widely consulted by government institutions and local authorities in connection with the planning of new legislative or program initiatives. These consultations have been a priority for this office. It means that the specialized resources concentrated in this office can be made available to many public bodies that do not currently have that kind of capacity.

To ensure our independence, we may only offer general, non-binding advice with the caveat that at some point we may receive a request to review an access decision or a breach of privacy complaint. At that time, we must proceed to deal with that business solely on the basis of full submissions from both the public body or trustee and the individual guided only by the evidence and submissions and the applicable law.

Enhanced Driver's Licence

In June 2008, we were consulted by Saskatchewan Government Insurance (SGI) with respect to its plan to develop an Enhanced Driver's Licence (EDL) that would meet the requirements of the Western Hemisphere Travel Initiative. We provided SGI with a copy of the joint resolution on EDL adopted by Canada's Privacy Commissioners in January 2008. That resolution included the following:

- "... 5. The Commissioners call on provincial and territorial governments to:
- a. ensure that individuals participate in an EDL program on the basis of informed consent, with full disclosure to individuals of all privacy-related matters before they consent;
 - b. ensure that robust privacy and security are built into all aspects of EDL projects, including by conducting thorough privacy impact assessments and threat risk assessments at the outset;
 - c. ensure that their EDL programs comply with applicable local privacy legislation; and
 - d. consult early and meaningfully with their privacy commissioner or other responsible privacy oversight official on all aspects of any contemplated EDL program."



The Freedom of Information and Protection of Privacy Act (FOIP)

Enhanced Driver's Licence (cont'd)

We requested and were assured in June and throughout the fall of 2008 that we would receive a detailed Privacy Impact Assessment (PIA) to review and comment on.

Before we received the detailed PIA, we learned of Bill 72, *The Traffic Safety Amendment Act*, that was undergoing debate by the Legislative Assembly in February 2009. As this Bill would enable the EDL, I determined that it would be important to raise those concerns we had already identified with the SGI initiative based largely on discussions that had already occurred in other Canadian jurisdictions throughout 2008. Our letter dated March 6, 2009 was presented as a report to the Legislative Assembly the same day. That letter is available on our website, www.oipc.sk.ca.

Our concerns with Bill 72 included the following:

1

Bill 72 made no reference to:

- radio frequency identification (RFID) tags;
- the privacy invasive character of RFID tags in this context;
- the risks to privacy associated with RFID tags;
- safeguarding the new database created by the EDL;
- an offence provision for failure to protect the personal information of EDL cardholders;
- penalties for failure to protect that personal information of EDL cardholders;
- any provision to mitigate the significant privacy risks; or
- any provision for the audit of the collection, use and disclosure practices of SGI associated with RFID tags or the personal information collected at the time of application for the EDL.



The Freedom of Information and Protection of Privacy Act (FOIP)

Enhanced Driver's Licence (cont'd)

- 2 Bill 72 failed to include many of the privacy protective features of Manitoba's EDL enabling legislation – *The Drivers and Vehicles Amendment, Highway Traffic Amendment and Manitoba Public Insurance Corporation Amendment Act*.
- 3 Bill 72 failed to address elements of privacy best practices and the Saskatchewan Overarching Privacy Framework for Executive Government.

In my report to the Legislative Assembly I provided ten specific recommendations to address our concerns with the EDL initiative.

Recommendations

- That Bill 72 be revised to explicitly recognize the privacy concerns associated with the EDL and that the Assembly should consider a number of privacy-positive features discussed in this submission.
- That Bill 72 be revised to specifically require that SGI take all reasonable measures to ensure the personal information collected, used or disclosed is adequately protected by means of physical, technical and administrative measures.
- That such a duty to safeguard information be reinforced by an offence provision and a serious penalty in the order of penalties in *The Health Information Protection Act*.
- That a detailed and thorough Privacy Impact Assessment be provided to our office without delay in order that we can provide our advice to the Assembly.



The Freedom of Information and Protection of Privacy Act (FOIP)

Enhanced Driver's Licence (cont'd)

Recommendations (cont'd)

- That the Assembly ensures that the radio frequency identification device utilized in Saskatchewan should be a proximity device instead of a vicinity device.
- That the Assembly consider the importance of ensuring that any consent associated with an application for an EDL or identity card be a fully informed consent.
- That the Assembly consider requiring that the EDL or identity card contain stronger security than that offered by the Faraday sleeve. Ideally, this would involve an on/off switch to be operated by the EDL or identity card holder.
- That Saskatchewan carefully considers the information and materials that have been developed in other jurisdictions, particularly Manitoba, and determine how those materials could be adapted for Saskatchewan.
- That any regulations, information tools, brochures be provided to our office in draft form in a timely way to enable us to provide input before roll-out of the EDL/identity card program.
- That any regulations be published in draft form to permit public comment before they are proclaimed.

Subsequent to our report to the Assembly, we did receive the PIA from SGI. We identified a number of questions and issues with respect to the PIA and supporting documents and on March 16, 2009 I wrote to the SGI Privacy Officer requesting further information.



The Freedom of Information and Protection of Privacy Act (FOIP)

Enhanced Driver's Licence (cont'd)

On March 26, 2009 the Minister responsible for SGI announced that Saskatchewan would not proceed with the EDL. In his statement, Minister Chevaldayoff stated that: *"Our government has been concerned for some time with factors including changing card requirements, unknown public demand for the card, privacy and security issues, start-up costs and costs going forward for many years for Saskatchewan, and the staffing requirements to deliver this program indefinitely."*¹⁶

Interestingly, the provinces of New Brunswick and Prince Edward Island then announced that they also would not proceed with the EDL. Alberta had announced in 2008 that it would not participate in the EDL program since it was too expensive and provided too little value to the relatively small number of citizens likely to apply for an EDL.

I commend the Saskatchewan Government for its quick action in cancelling the EDL program and instead encouraging all Saskatchewan residents to obtain a passport prior to June 1, 2009 when it will be required to drive into the United States.

Administrative Tribunals and the Internet

Our office issued its Investigation Report H-2005-001 in 2005. At that time the Saskatchewan Automobile Injury Appeal Commission determined that it would not accept our recommendations that the names of residents be masked if the decisions of the Commission were to be published to the world on the Internet.

As noted in last year's Annual Report, effective June 1, 2008 the Commission reversed its position and accepted our recommendations from Report H-2005-001.

Since that time, the federal Privacy Commissioner has taken the same approach in a number of cases it dealt with in the summer of 2008. There has been considerable interest from the Canadian Bar Association and administrative tribunals both within and outside of Saskatchewan in this issue.



The Freedom of Information and Protection of Privacy Act (FOIP)

Administrative Tribunals and the Internet (cont'd)

Currently, we are surveying all Saskatchewan administrative tribunals on their Internet publication practices and what steps they have taken or are prepared to take to address the legitimate privacy concerns of citizens.

We have developed an extensive resource list in respect of the question of administrative tribunals and Internet publication of decisions.

Finally, in collaboration with Privacy Commissioners in other Canadian jurisdictions, our office is working on a set of guidelines for administrative tribunals to assist them in addressing privacy concerns associated with Internet publication.

Privacy Impact Assessment for Saskatchewan Laboratory Results Repository (SLRR)

A major advice and consultation file was the review of the detailed PIA done by Saskatchewan Health for a domain repository of the developing electronic health record (EHR). This is discussed further in the HIPA portion of this Annual Report on page 28.



The Freedom of Information and Protection of Privacy Act (FOIP)

TOOLS AND PUBLICATIONS

Consistent with our mandate to promote understanding of access and privacy laws in Saskatchewan, we have produced a number of materials during the 2008 - 2009 fiscal year. These include:

- ***Privacy Breach Guidelines*** - this resource highlights the six sequential steps to be taken by organizations when they discover a privacy breach
- ***Annotated Section Indexes for The Freedom of Information and Protection of Privacy Act, The Local Authority Freedom of Information and Protection of Privacy Act and The Health Information Protection Act***
- ***Annotated Section Index for Investigation Report H-2005-002***
- ***Resource List for Administrative Tribunals and Internet publication of decisions***
- **Maps displaying:**
Access and Privacy Laws across Canada
Federal access and privacy laws
Access and Privacy Oversight offices across Canada
- **Slide deck and resource list for Brown Bag Luncheons:**
How to Survive as a FOIP/HIPA Coordinator
Severing Made Easy
- **Personal Information Retained by Office Machines** (backgrounder)

All of these materials are available on our website at www.oipc.sk.ca.



The Freedom of Information and Protection of Privacy Act (FOIP)

Right to Know

Our office has been a proud partner with a number of other Saskatchewan organizations in planning activities during the last week of September to commemorate Right to Know Week for three consecutive years. This is tied to September 28, the Right to Know Day recognized in many of the 60 nations around the world that have an access to information law. The designation of Right to Know Week emphasizes the value of the right of individual access to information held by public bodies and marks the benefits of transparent, accountable government. Each year, Right to Know Week has been recognized by a number of events held in Saskatoon and Regina.

The benefits of access to information highlighted during this week include:

- providing individuals with knowledge to address public issues, scrutinize government and become active participants in the democratic process.
- revealing and clarifying the basis for government decisions, disclosed environmental and health dangers and shed light on error, mismanagement and illegal activities.
- requiring improved records management, prompted routine disclosure of information, promoted the duty to assist the public and resulted in better government service and efficiencies.

Formal proclamations were issued by the cities of Regina and Saskatoon as well as the Saskatchewan Government.

The Regina Public Library showed films during the week related to the public's right to know. The films included: *Standard Operating Procedure*, *This Film is Not Yet Rated* and *Boy-A*.



The Freedom of Information and Protection of Privacy Act (FOIP)

Right to Know (cont'd)

The keynote presentation in Regina was delivered by Professor Alasdair Roberts who is the Jerome L. Rappaport Professor of Law and Public Policy at Suffolk University Law School. The topic of his presentation was *Blacked Out - Government Secrecy in the Information Age*.

The keynote presentation in Saskatoon was delivered by Ms. Suzanne Legault, Assistant Information Commissioner of Canada. The topic of her presentation was *Modernizing Access to Information in Canada: From Town Crier to the Global Village*.

The Culliton Award is presented each year to a public body which demonstrates strong leadership in promoting the public's right to access public records. This award was presented to Ms. Darlene Eberle, Chairperson of the Saskatoon Health Region.

High school and university or college students were invited to enter an essay contest on the topic: *Why the right of access to information is important in a modern democratic society*. Winners of the essay contents received cash prizes. The \$500 cash prize was awarded to a student of the University of Regina and the \$300 cash prize was awarded to Anna Bigland-Pritchard of Borden, Saskatchewan.

The week's events were supported by the Canadian Bar Association, Johnson Shoyama Graduate School of Public Policy, Law Foundation of Saskatchewan, McKercher McKercher & Whitmore LLP, McPherson Leslie & Tyerman LLP, Regina LeaderPost, Regina Public Library, Saskatoon StarPhoenix and the Sheldon Chumir Foundation for Ethics in Leadership.



The Local Authority Freedom of Information and Protection of Privacy Act (LA FOIP)

My previous comments, with respect to government institutions, would apply to local authorities as well. This is an area where there is a great need for resources and assistance to achieve LA FOIP compliance.

Recent efforts by the Access and Privacy Branch to offer workshops, and to modify its online learning program for local authorities have been encouraging. What is missing is a statutory requirement equivalent to section 63 of FOIP:

“63(1) The minister shall prepare and submit an annual report to the Speaker of the Assembly on the administration of this Act and the regulations within each government institution during the year, and the Speaker shall cause the report to be laid before the Assembly in accordance with The Tabling of Documents Act.

(2) The annual report of the minister is to provide details of:

(a) the number of applications received by each government institution during the year;

(b) the number of times during the year that the head of each government institution refused an application for access to a record, and the specific provisions of this Act or the regulations on which the refusals were based; and

(c) the fees charged and collected by each government institution for access to records during the year.

(3) The minister may require government institutions to produce the information or records that, in the opinion of the minister, are necessary to enable the minister to fulfil the requirements of this section.” [emphasis added]

As a result, there is no requirement for any kind of annual report that conveys useful information on the activities and practices of local authorities that would be equivalent to the annual report required from Justice in respect of government institutions.

Also, there is no rational need in 2009 for a separate statute for local authorities and I renew my earlier recommendation that it be fully integrated into a single FOIP Act as is the case in all jurisdictions other than Ontario and the federal level.



The Health Information Protection Act (HIPA)

As we move towards the EHR, there will need to be more recognition of the limitations in the protection afforded by HIPA. Although we do not yet have comprehensive EHRs for all patients, we are steadily moving in that direction. A good deal of patient information is now stored digitally. Patients are entitled to assess how well trustees are doing in protecting their information now in our partly paper and partly electronic systems. This is relevant to understanding the degree of confidence we can invest in our future EHR system. In other words, if we cannot do an adequate job at this time, why would we expect higher standards tomorrow when we have a fully functioning EHR system?

It is true that there are very large penalties provided for violation of HIPA and that the EHR system being constructed in Saskatchewan appears to have an ability to audit uses and disclosures of EHR data. The experience in Canada with laws like HIPA is that those provisions may not be sufficient to ensure statutory compliance. For example, the offence provision is used rarely. To our knowledge there have been only two prosecutions in the last 10 years. One occurred in Manitoba and resulted in an absolute discharge. The other occurred in Calgary and resulted in a \$10,000 fine.

Audits by definition are retrospective and may catch breaches of HIPA but this may be of little comfort to the individual whose personal information has been improperly used or disclosed without his/her consent. In any event, we are not comfortable that all of the larger trustee organizations have a routine audit protocol that entails regular surveying of use and disclosure practices as opposed to simply having that capability.

What safeguards are trustees installing with respect to electronic record systems to actually prevent the prospective breach? The safeguards appear primarily to be three:

- 1** Requirement for staff to enter into a confidentiality agreement
- 2** Policies and procedures
- 3** Training



The Health Information Protection Act (HIPA)

These three measures may not be sufficient in light of the following experience with trustees to date:

- 1 We have encountered a number of cases where breaches have occurred by reason of improper use or disclosure of personal health information by persons who have executed a confidentiality agreement.
- 2 Regional Health Authorities should now have a full range of policies and procedures to comply with HIPA. Nonetheless, we have seen cases where those policies have been violated by employees of health authorities.
- 3 Training has been provided by Regional Health Authorities to their staff. Here again, this has been insufficient given breaches that have occurred to date. For example, in one region the very health records staff responsible to provide the HIPA training to other regional staff improperly viewed personal health information of a patient in clear violation of HIPA, their own training, their confidentiality agreement and their Region's policies and procedures.

HIPA requires, among other things, that a trustee must establish policies and procedures to maintain administrative, technical and physical safeguards that will protect against any "reasonably anticipated" unauthorized access to, use or disclosure of personal health information.

This means that Saskatchewan trustee experience to date helps determine what risks are "reasonably anticipated." It follows that all trustees will need to assess what further steps should be taken since our experience to date is that inadequacies are being identified with existing systems. I am encouraging trustees to reassess the "role-based" use model now employed and assess how it can be narrowed and strengthened.



The Health Information Protection Act (HIPA)

I continue to have concerns with certain features of the EHR under construction in this province. Two chief concerns were first discussed in my 2007-2008 Annual Report:

- accountability; and
- compulsory uploading of all patient information to the system.

ACCOUNTABILITY

On the accountability question, we have observed the progress made by the Health Information Solutions Centre (HISC) with the third domain registry in the province – the Saskatchewan Laboratory Results Repository (SLRR). Unfortunately, the accountability issue is still not being adequately dealt with. In fact, the approach we criticized one year ago is still evident in SLRR and is apparently being replicated in each of the domain repositories as they are being rolled out. This approach is to rely on agreements between trustees that assign different responsibilities to different trustees. In some cases, certain governance responsibilities are even assigned to non-trustees such as the Governance Committee. The web of agreements that purport to address accountability are opaque to the individual patient/client. I continue to encourage Saskatchewan Health to ensure a simpler and clearer accountability structure consistent with the preamble to HIPA.

COMPULSORY (NON-CONSENTED) UPLOADING

In my last Annual Report, I asserted that Saskatchewan residents are entitled to a measure of control over their own personal health information. This would take the form of allowing patients the right to request that their primary provider refrain from uploading certain personal health information to the EHR. In my experience, it is unlikely that a large number of persons will choose to exercise such a right and I fully expect that the vast majority of residents will be comfortable uploading all of their information to the EHR. The right of privacy, however, is very much an individual right and it is singularly inappropriate for any trustee, no matter how well-intentioned, to ignore the wishes of their patient in the event that patient has had for example an abortion, a mental health illness or some matter they consider highly prejudicial to them. I continue to urge Saskatchewan to develop a feature that will allow certain information to be retained by the patient and their primary provider and not require all information to be forwarded to the EHR.



The Health Information Protection Act (HIPA)

SECONDARY USES AND DISCLOSURES

Health privacy law and practice recognizes that personal health information is provided by the patient to the care provider for a primary purpose, namely, for their diagnosis, treatment and care. It is well recognized that express consent is not required from the patient when he or she presents at a health care facility seeking diagnosis, treatment or care. It is further recognized that there are multiple other uses and disclosures that health providers and health administrative bodies apply to that same information. Generally, these multiple other uses and disclosures, independent of the diagnosis, treatment and care of the patient, are recognized and described as secondary purposes.

A good example of 'function creep' and expanded secondary use of personal health information are developments with respect to the Saskatchewan Health Services Number and card. The original purpose was to establish coverage for an individual under our health insurance plan. Over time it has become so widely demanded and used for so many other purposes, it almost appears to have become a de facto provincial identity card. For example, many agencies both public and private routinely request that people provide their health services card to obtain all kinds of services unrelated to the provision of health care.

A recent example are the new rules for Saskatchewan lawyers ostensibly for purposes of deterring money-laundering activities.¹⁷ Lawyers will now be expected to require the production of identity documents such as the health services card, make a copy and retain that copy until the scheduled destruction date of the client's file. Section 11 of HIPA attempts to restrict the use of the health services number to health care delivery. Presumably the purpose of section 11 of HIPA was to ensure that widespread demands for production and collection of copies of health services cards would undermine confidence of patients in the security of their personal health information in an EHR world. I urge Saskatchewan Health to consider communication strategies to raise awareness of section 11.



The Health Information Protection Act (HIPA)

TOO MANY PRIVACY BREACHES

Our office has received a distressingly large number of complaints and alerts with respect to privacy breaches by Saskatchewan trustees. Notwithstanding section 16 of HIPA, we are finding too many trustees that do not have written policies and procedures for administrative, technical and physical safeguards to adequately protect the personal health information they routinely collect, use and disclose. There have been problems with surplus equipment being disposed of without health information being purged, programmed fax numbers that have not been updated, lost or stolen mobile security devices such as laptop computers and personal health information blowing around on streets. Despite numerous reminders from our office, and the publication of tools available on our website, we see no abatement in the volume of complaints.

PRAIRIE HEALTH INFORMATION DAY

For the second consecutive year, our office co-sponsored, with the Information and Privacy Commissioner of Alberta and the Manitoba Ombudsman, a one day conference on health information laws and practices in the three prairie provinces. Topics included Recent Cases: Stories from the Trenches; EHRs; Current Debates and Future Considerations; Current Issues with managing Access Requests; Friends, Family, Surrogates . . . Access or Disclosure and Information Management Agreements with Third Party Contractors. Many of the presentations are available online at www.verney.ca/hipd2008/agenda.php.



Use of Privacy Impact Assessments

I am very encouraged to see more use of Privacy Impact Assessments¹⁸ (PIA) by organizations that we oversee. In 2005, we published on our website PIA forms for each of the three laws that this office oversees. Now that it is a more familiar tool, it is perhaps timely to revisit its utilization and how it can be optimized. It is important that someone outside of the business unit developing the program in question be involved in the PIA process. Otherwise, there is often a lack of rigor since there is such a strong vested interest in finding that the proposed program or activity is compliant. Too often there is little regard to privacy best practices. This is problematic since our first-generation FOIP and LA FOIP statutes are quite weak instruments for the purposes of privacy protection. It becomes important to identify whether the proposed program not only matches what may be very minimal statutory requirements, but whether it is consistent with higher privacy best practices that have now been codified in most modern privacy laws in Canada.

Too often PIAs are focused too broadly and fail to come to terms with the granular operation of a proposed program. We find that the use of a detailed data flow chart helps the reader as well as the authors of the PIA. That serves to more clearly identify what personal information is in play, what collections, uses and disclosures are anticipated and then what statutory provisions must be satisfied.

We have often been critical of a lack of rigor and clarity in the analysis of consent and accountability and secondary uses and disclosures of personal information in PIAs that we have had the opportunity to review. For example, in one PIA our office reviewed we found the assertion that the program under HIPA would *"operate on a deemed consent model which focuses on implied consent from a policy perspective"*. Our advice to the trustee in question was that such an assertion was incomprehensible. It is always important that a reader who does not have a detailed understanding of a program subject to a PIA can pick up the PIA and be able to comprehend what is proposed and the extent to which it conforms or fails to conform to legislation and privacy best practices.



National Meeting of Oversight Agencies held in Saskatchewan

On June 3 - 5, 2008 our office hosted the very first annual meeting of Information and Privacy Commissioners and Ombudsmen in our province. In association with that meeting, our office recruited and organized a meeting with a group of 'tech-savy' students from Moose Jaw who discussed with the Commissioners their experience and knowledge of privacy issues related to social networking.

This led to a unanimous resolution adopted by all Commissioners addressing privacy challenges associated with social networking. Part of that resolution is as follows:

"IN THIS CONTEXT, CANADA'S PRIVACY COMMISSIONERS AND PRIVACY ENFORCEMENT OFFICIALS ("COMMISSIONERS") RESOLVE AS FOLLOWS:

The Commissioners will work together to implement public education activities meant to increase awareness among children and young people of the privacy risks inherent to their online activities.

The Commissioners recommend to governments, industry, child and youth advocates, ombudsmen and other institutions and organizations dedicated to improving children's well-being to work in partnership to develop and disseminate public education tools to individuals who work with and influence children every day, including their parents, care providers and teachers.

The Commissioners responsible for private sector privacy laws (Alberta, British Columbia, Quebec and Canada) urge industry to adopt the highest standard of privacy possible when developing online environments targeted at children and young people.

The Commissioners urge operators of websites created for children and young people to demonstrate their social responsibility in adopting privacy policies and usage agreements that are clear, simple, and understandable to the user, and educating their users of existing privacy and security risks.



National Meeting of Oversight Agencies held in Saskatchewan

The Commissioners will develop guidance for industry to assist operators of websites for children and youth in the development of better privacy practices. Children and young people should expect that organizations operating online environments comply with privacy laws. If they believe their personal information has been mishandled, they have the right to lodge a complaint with the appropriate commissioner and seek resolution.

Finally, Canadian Commissioners wish to work with data protection regulators from other countries to ensure that children and young people around the world have access to a safe online environment respectful of their privacy."

As a result of that initial work, there is now an ongoing collaboration between Children's Advocates offices and Privacy Commissioners dealing with this issue.



Growing Public Awareness

I have been very encouraged by the evident growth in awareness of privacy and access issues by both public bodies, trustees and the public. This is manifest in certain areas of service of our office.

We received approximately 3100 telephone calls or email inquiries about access and privacy laws in Saskatchewan and for assistance in dealing with them. This represents an increase of 12% over the previous year. We are encouraged that more MLA constituency offices are referring the public to our office for assistance than in previous years.

We have received strong positive feedback from members of the public as well as from public bodies and trustees that our free e-newsletter, the *Saskatchewan FOIP FOLIO*, is a useful resource. There are now 58 (as of April 1) past issues archived on our website. This has been effective in alerting readers to new privacy and access developments in our province and beyond, to best practices and to our ongoing reports and recommendations.

In the 2008 - 2009 fiscal year, we opened 69 detailed advice and commentary files. These represent requests from the bodies we oversee for assistance in assessing new projects or proposed legislation for statutory compliance and 'best practices'.

We have been contacted by members of the public who are interested in attending the Brown-Bag lunch hour workshops on FOIP and HIPA compliance. These workshops are offered currently to FOIP and HIPA Coordinators and Privacy Officers only. We plan in the future to offer some workshops specifically designed for the public.

Finally, our website, www.oipc.sk.ca continues to attract more visitors. During the 2008 - 2009 fiscal year we attracted 322,317 hits. That represents an increase of 19% over the previous fiscal year.



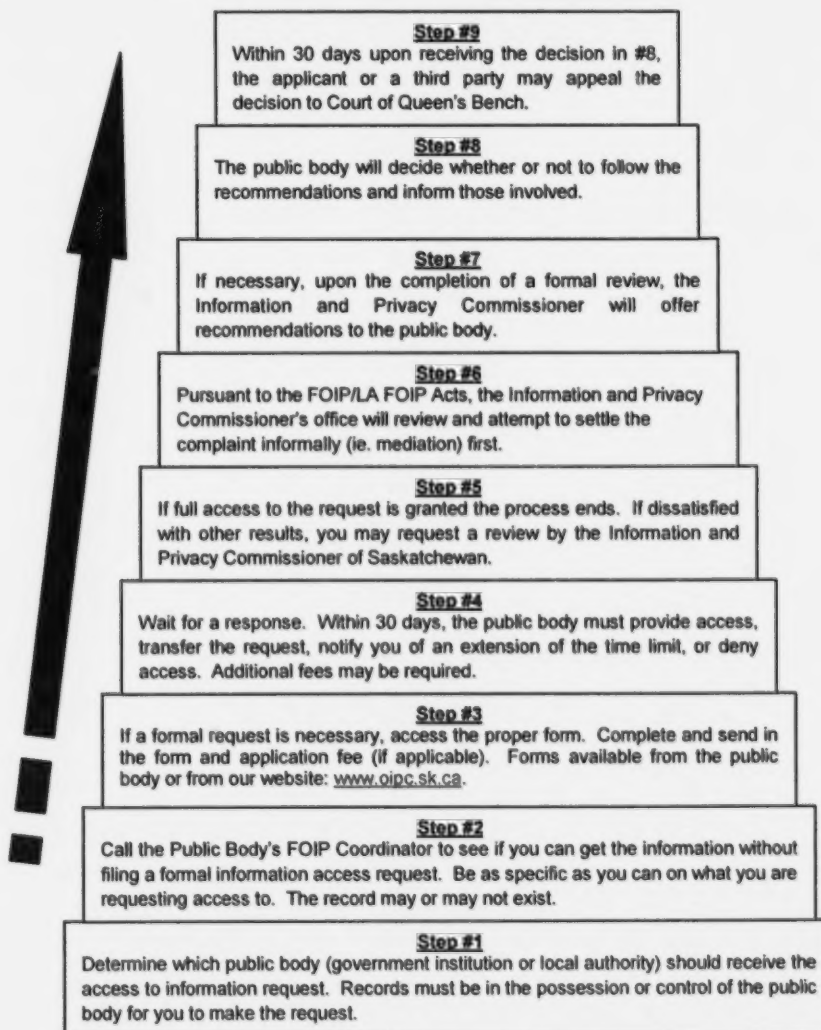
Capacity of the OIPC

For the 2008 - 2009 fiscal year, in addition to the Commissioner, there was approval by the Board of Internal Economy for six FTEs in total but only for three Portfolio Officers. All of the intake, investigations and reviews are undertaken by the Director of Compliance and the Portfolio Officers. As a result, we have effectively had only the Commissioner, Director of Compliance and one fully trained Portfolio Officer to close files.

The lack of capacity in terms of investigations and reviews translates directly into unacceptable delays for citizens who are attempting to assert their information rights guaranteed to them by statute. We have not been able to achieve those key performance measures in our Business Plan related to investigations and reviews. This gap between our workload and our capacity to do our investigative and review work grows larger with the dramatic increase in breach of privacy complaints noted earlier.



How to Make an Access Request



How to Make a Privacy Complaint

1. The complainant should first contact the Privacy Officer or FOIP Coordinator for the government institution, local authority or trustee (the public body) to attempt to resolve the complaint.
2. If no satisfactory resolution of the concern is reached by dealing directly with the public body, the complainant may choose to file a written complaint with the Information and Privacy Commissioner.

Generally, the Office of the Information and Privacy Commissioner (OIPC) will not deal with a complaint that is two years old or older.

The complaint should be in writing and should provide the following:

- complainant's name, address and phone number;
- date;
- specific government institution, local authority or trustee against whom the complaint is made;
- copies of any correspondence with the public body relevant to the complaint;
- description of the events giving rise to the complaint; and
- clarify whether the complainant wishes to be treated as anonymous when the OIPC communicates with the public body.



How to Make a Privacy Complaint

3. Once we review the complaint the following will occur:

- Once it is determined that the OIPC has jurisdiction to investigate, a Portfolio Officer will be assigned to the file.
- The Portfolio Officer will advise the public body of the complaint and that the OIPC will be investigating under the authority of FOIP, LA FOIP or HIPA. At the same time, we will advise the complainant that an investigation is underway.
- Once it is determined that the OIPC has jurisdiction to investigate, a Portfolio Officer will be assigned to the file.
- The Portfolio Officer will advise the public body of the complaint and that the OIPC will be investigating under the authority of FOIP, LA FOIP or HIPA. At the same time we will advise the complainant that an investigation is underway.
- The Portfolio Officer will gather information from the public body to determine the relevant facts.
- The Portfolio Officer will define the issues for purposes of the investigation and invite submissions from the public body and the complainant.
- The Portfolio Officer will attempt to mediate, or otherwise informally resolve the complaint, with complainant and public body.
- If no mediated settlement is possible, the Commissioner will proceed to issue a formal Investigation Report. The identity of the complainant will not be disclosed.
- There may be a limited right of appeal to the Court of Queen's Bench by an aggrieved complainant if the complaint was handled under HIPA pursuant to section 46. No right of appeal from a report dealing with a breach of privacy under FOIP or LA FOIP.



Case Summaries

In 2008 - 2009, 97% of the review and complaint files we closed resulted from an informal resolution of the access request or privacy complaint and did not therefore result in the issuance of a formal report. This represented 76 files closed in 2008 - 2009.

REPORT F-2008-002 (MINISTRY OF JUSTICE AND ATTORNEY-GENERAL)

A request for copies of any minutes of meetings from the Funeral and Cremation Services Council (Council) was submitted to the Superintendent of Funeral and Cremation Services (Superintendent) at the Consumer Protection Branch, an agency of the Department of Justice. The Department of Justice responded that it did not have such a record in its possession. The issue under review was whether the responsive record, even if not in Justice's possession, was nonetheless in its control.

The focus of the analysis was on section 5 of *The Freedom of Information and Protection of Privacy Act* (FOIP). I found that, of the factors recognized in other jurisdictions, none existed in this case to render the Council's records under the 'control' of Justice. I further found that *The Funeral and Cremation Services Act* (FCSA) creates a system whereby the Council operates independently from Justice in its management of the licensees under the FCSA, and that the Superintendent acts largely as an oversight body. This involves the consideration of appeals from Council decisions and other matters that pertain to the administration of the FCSA. As such, I found that it is not reasonable for meeting minutes of the Council to be considered to be under the control of Justice.

The Ministry advised our office that it decided to follow our recommendation and take no further action on the request for access.



Case Summaries

REPORT H-2008-002**(DR. VAL MARY HARDING, CARRYING ON BUSINESS AS HARDING
PSYCHOLOGICAL SERVICES AND ALSO LEBELL & ASSOCIATES)**

The Applicant attended on Dr. Harding, a Regina psychologist, for purposes of an independent medical examination (IME) in the form of a psychological assessment, at the request of the Applicant's employer. Before commencing the IME, Dr. Harding received a five page letter from a third party dated March 12, 2007 (the March 12, 2007 letter). This letter contained personal health information concerning the Applicant and also a number of prejudicial statements about the Applicant. Dr. Harding denied access to the March 12, 2007 letter and personal health information in other documents concerning the Applicant. She did so citing section 38(1)(a) of *The Health Information Protection Act* (HIPA) (reasonable expectation of injury to any person) and section 38 (1)(c) of HIPA (disclosure of identity of source of confidential information).

I determined that the Applicant was entitled to access his personal health information in Dr. Harding's file including the March 12, 2007 letter subject to appropriate severing. I recommended that portions of the letter be severed on account of information that did not qualify as 'personal health information' and other portions on account of the requirement to not disclose the source of confidential information supplied by a third party.

Dr. Harding advised our office that she accepted our recommendations and that she would release to the Applicant both the psychological assessment and the third party letter severed in accordance with our recommendations.



Business Plan, Budget & Statistics

BUSINESS PLAN, BUDGET & STATISTICS

When I started my first term, I adopted a practice of developing and publishing business plans for a three year period. Each plan included priority actions and key performance measures.

My Business Plan for 2007 - 2009 describes 5 core businesses of the OIPC, 12 specific goals for the OIPC and 23 different key performance measures for 2008-2009. We distributed this Business Plan to all members of the Assembly then published on our website, www.oipc.sk.ca in early January 2008.

We can summarize achievement in respect of those 23 key performance measures for the current fiscal year (April 1, 2008-March 31, 2009) as follows:

Exceeded:	5
Achieved:	7
Partially achieved:	7
Not achieved:	<u>4</u>
Total:	23

We closed 76 case files (review and breach of privacy) in this fiscal year. However, once again, our most serious failing is in consistently moving reviews and investigations to mediation stage or report in a more timely fashion. As indicated earlier though, our office has had to contend with an increase in demand for our services and high degree of employee turnover that has inhibited our ability to make more of an impact in this regard.

Reasons for this failure to achieve targets for dealing with our body of reviews and investigations are described on page 35.



Business Plan, Budget & Statistics

Measuring up

Our Business Plan for 2008-2009 includes the following five core businesses:

- Core Business 1:** Reviews of decisions on access requests
- Core Business 2:** Reviews of breach of privacy complaints
- Core Business 3:** Trustee/Government Institution/Local Authority Compliance
- Core Business 4:** Clarifying the Access and Privacy Regime in Saskatchewan
- Core Business 5:** Public Education

It also included 12 specific goals and 23 different key performance measures for this past fiscal year. A more detailed assessment of those key performance measures follows.

Performance measures for 2008 - 2009

EXCEEDED

Explore with Privacy Commissioner of Canada opportunities to collaborate in creation of public education materials and presentation of information to the public

We have collaborated with the Privacy Commissioner of Canada in the development of its new program – *Privacy Made Simple* which was rolled out exclusively in Saskatchewan in 2008 - 2009. This entailed the creation of educational materials and tools for small and medium sized businesses and for the Saskatchewan public. One of the objectives is to reduce the high volume of calls to the OIPC seeking assistance with compliance with the federal *Personal Information Protection and Electronic Documents Act*. Another purpose is to raise public awareness of privacy principles common to both federal and provincial legislation.



Business Plan, Budget & Statistics

Performance measures for 2008 - 2009 (cont'd)

EXCEEDED

Ensure that 90% of all requests for summary advice from government institutions, local authorities, and trustees receive a response within 72 hours.

We routinely achieve the above in more than 90% of requests. More than one half of such requests were answered within 24 hours.

Ensure that 90% of summary advice for citizen requests within 72 hours.

We routinely achieve this in more than 90% of requests. We respond to more than one-half of such requests within 24 hours.

Ensure that education presentations are made available to a wide variety of audiences in a number of different Saskatchewan communities.

Education sessions provided in the current fiscal year to date in Saskatchewan exceed 125 in various communities throughout the province. Appendix II is a sample list of such presentations.

Ensure that educational presentations on the review and investigation process have been completed for every Ministry, every Crown corporation, every provincial board and agency, every school division, all urban and rural municipalities, every health region and every university or college that has requested a presentation.

We have met this objective, although in one case we could not resolve a scheduling conflict in order to participate in a teacher's convention in one division. In a number of other cases, we have had to delay the presentations because of insufficient number of presenters in our office.



Business Plan, Budget & Statistics

Performance measures for 2008 - 2009 (cont'd)

ACHIEVED

Create a section index of all published review reports done by the OIPC.

Annotated Indexes for FOIP, FOIP Regulations, LA FOIP, LA FOIP Regulations, HIPA, and HIPA Regulations are available on our website, www.oipc.sk.ca. In addition, we have created a separate section index for Investigation Report 2005 - 002 since it was our first Investigation Report under HIPA and included interpretation of many sections of HIPA.

Host 'Brown-Bag' luncheon workshops on access and privacy compliance for access and privacy coordinators in government institutions, local authorities, and trustees.

Two Portfolio Officers have been tasked with responsibility for a series of luncheon workshops in the first three months of 2009. Topics include: How to Survive as a FOIP Coordinator, How to Sever, and Duty to Assist. We advertised these sessions in the January 2009 *FOIP FOLIO*.

Publish advisory material to address areas of concern and confusion among government institutions, local authorities, and trustees.

This includes our monthly e-newsletter entitled the *Saskatchewan FOIP FOLIO*, maps of federal, territorial, and provincial Information Access and Protection of Privacy Laws and oversight offices, *Privacy Breach Guidelines*, paper titled *Administrative Tribunals, Privacy and the Net*, and *Backgrounder on Personal Information Retained by Office Machines*.



Business Plan, Budget & Statistics

Performance measures for 2008 - 2009 (cont'd)

ACHIEVED

Provide commentary in the 2007 - 2008 Annual Report on clarifying the access and privacy regime in Saskatchewan.

The Annual Report included a 13 page analysis of specific challenges surrounding HIPA and roll out of the EHR with specific recommendations to the Assembly for remedial action. The OIPC has provided extensive material to the Government of Saskatchewan on the kinds of legislative review and legislative change to FOIP type legislation either implemented or considered in other Canadian jurisdictions. This was presented as Appendix I.

Encourage public bodies to make stronger commitments, through leadership initiatives, to achieve full statutory compliance.

In the current fiscal year, our office has had meetings with the CEO and Board of the Health Quality Council, the President and CEO of the Saskatchewan Medical Association, and the Saskatchewan Medical Association Representative Assembly to strengthen statutory compliance (HIPA). The Commissioner presented to representatives of all of Saskatchewan's health regulatory bodies and colleges on changes to improve HIPA compliance. In late 2008, the Commissioner met with the Board of the Cypress Regional Health Authority to discuss the governance challenge associated with HIPA.

Produce additional brochures on access and privacy issues for citizens.

We have added a Fraud Awareness (Identity Theft) section on our website, and expanded the Right to Know section on our website.



Business Plan, Budget & Statistics

Performance measures for 2008 - 2009 (cont'd)

ACHIEVED

Continue to participate in the planning of future 'Right to Know' events and to assist the Saskatchewan Right to Know Committee in organizing Right to Know Week in 2008.

In the current fiscal year, our Administrative Coordinator served as the Coordinator for RTK committee activity. The OIPC hosted meetings of the Saskatchewan Right to Know Committee, arranged for proclamations from the Government of Saskatchewan, the cities of Regina and Saskatoon and prepared the printed program for the events in Regina and Saskatoon. The OIPC arranged for Professor Roberts (Suffolk University) and Assistant Commissioner Suzanne Legault (Office of the Information Commissioner of Canada) to come to Saskatchewan and speak at the two major events in Regina and Saskatoon.

PARTIALLY ACHIEVED

By January 1, 2009, 80% of all new reviews to mediation or report stage within five months.

Given the substantial backlog and the delays discussed earlier along with insufficient personnel, we did not fully accomplish this goal.

By January 1, 2009, 60% of all investigations to report stage within five months.

Same as above.



Business Plan, Budget & Statistics

Performance measures for 2008 - 2009 (cont'd)

PARTIALLY ACHIEVED

Complete all pending reviews that are more than one year old.

In the current fiscal year, the OIPC has closed 31 review files that are more than one year old. The breakdown of review files at least one year old from each fiscal year closed this fiscal are as follows:

2004-2005 – 4 case files
2005-2006 – 3 case files
2006-2007 – 14 case files
2007-2008 – 10 case files

Publish at least 10 reports from reviews on the OIPC website.

I issued two Review Reports (F-2008-002, H-2008-002) and published on our website, www.oipc.sk.ca in the current fiscal year.

We will undertake 10 site visits to trustee facilities.

The OIPC does not have sufficient Portfolio Officers to achieve this performance measure. Only one site visit took place in the current fiscal year. The OIPC team toured the Cypress Regional Health Authority in April, 2008 visiting six different trustee facilities within that region.



Business Plan, Budget & Statistics

Performance measures for 2008 - 2009 (cont'd)

PARTIALLY ACHIEVED

We will undertake 10 site visits to government institutions and local authorities.

The OIPC does not have sufficient Portfolio Officers to achieve this performance measure. We visited the Regina Provincial Correctional Centre, toured the facility, and met with senior staff in the fall of 2008.

Provide commentary and advice through reports to the Legislative Assembly.

On March 6, 2009, I provided commentary to the Assembly on Bill 72, *The Traffic Safety Amendment Act*. A copy of that letter is available on our website, www.oipc.sk.ca under the *What's New* tab.

NOT ACHIEVED:

We will produce annual 'report cards' on government institutions that serve to highlight their response to access requests.

Collaborate with appropriate government institutions, local authorities, and trustees to develop Frequently Asked Questions (FAQs).

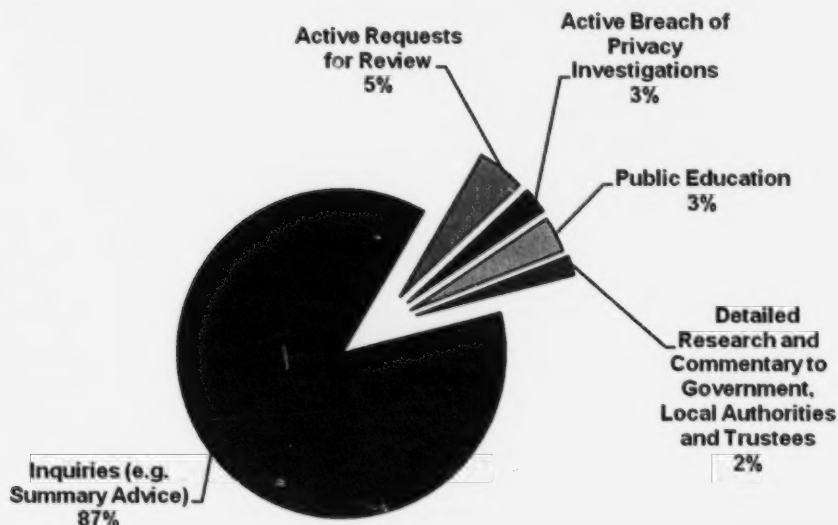
Participate in national 'Right to Privacy Day' events in 2008.

Publish a report on at least one office-initiated investigation.

A statistical review of our work in 2008 - 2009 follows.



Distribution of Requests for Service 2008-2009

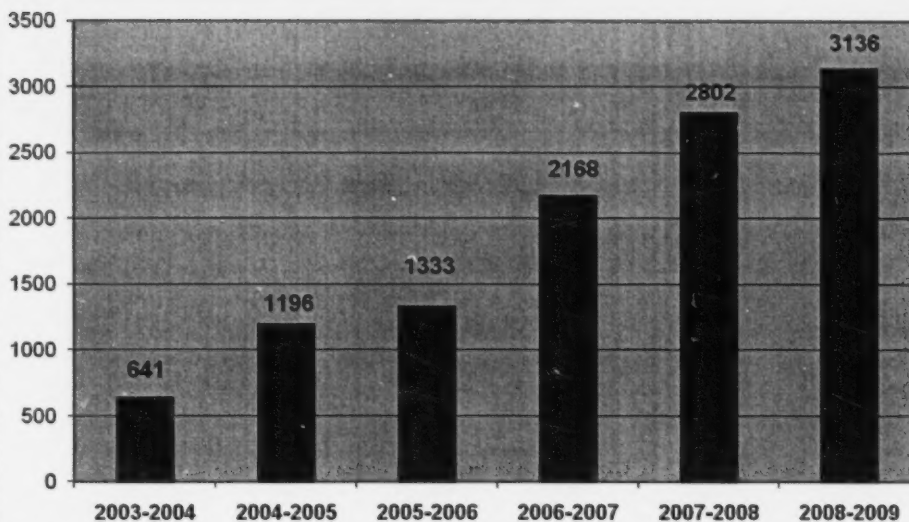


Description	2007-2008	2008-2009
Active Requests for Review Files	127*	170*
Active Breach of Privacy Investigation Files	66*	91*
Public Education	82	126
Detailed Research and Commentary to Government, Local Authorities and Trustees	66	69
Inquiries (e.g. Summary Advice)	2802	3136
Total	3143	3592

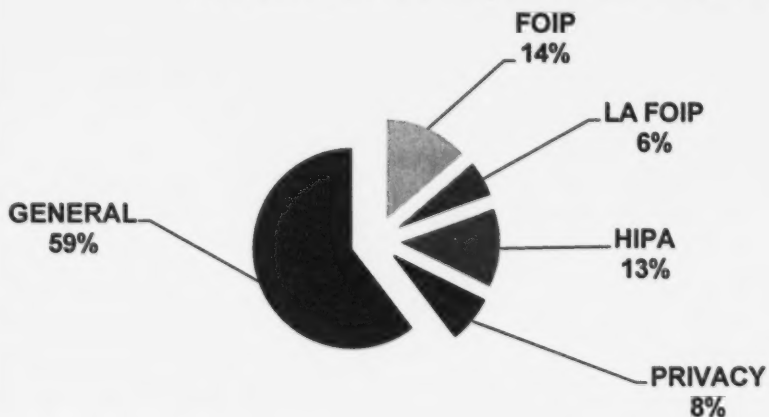
* Number is representative of open files carried over from previous years, as well as those opened during the fiscal year indicated.



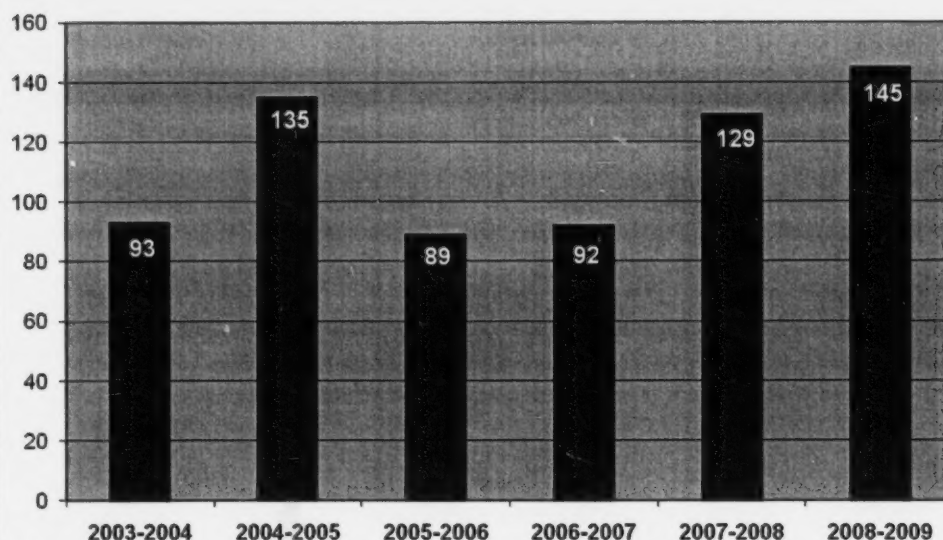
Inquiries by Fiscal Year



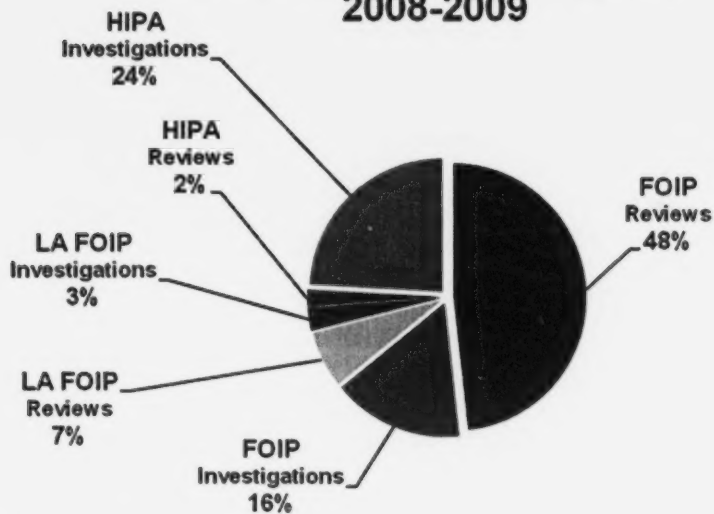
Breakdown of Inquiries 2008-2009



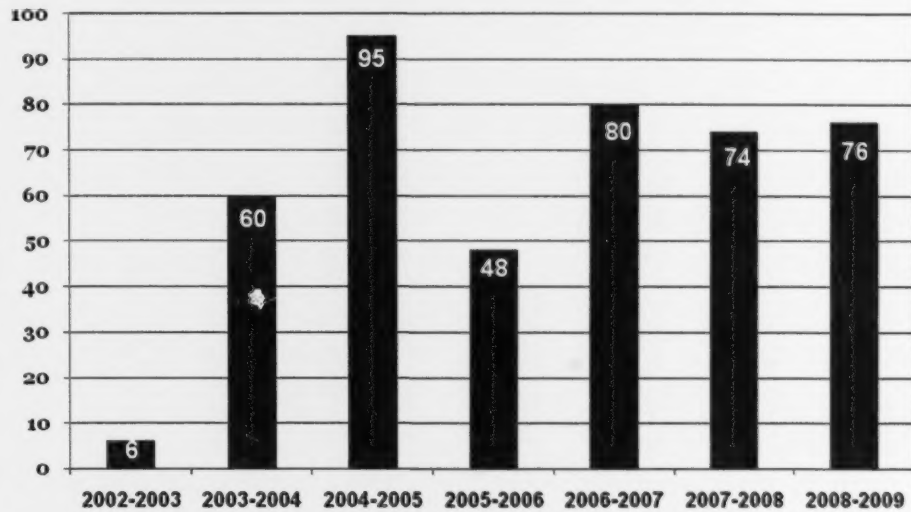
Case Files Opened per Fiscal Year



Breakdown of Files Opened 2008-2009

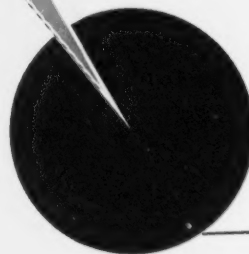


Case Files Closed per Fiscal Year



Case Resolution 2008-2009

Report
Rendered
3%



Informal
Resolution
97%



**Responses to Reports Rendered
2008 - 2009**

**Institution
Complied With All
Recommendations
100%**



FINANCIAL STATEMENTS

For the Year Ended March 31, 2009







SASKATCHEWAN

Provincial Auditor Saskatchewan

1500 Chateau Tower
1920 Broad Street
Regina, Saskatchewan
S4P 3V2

Phone: (306) 787-6398
Fax: (306) 787-6383
Web site: www.auditor.sk.ca
Internet E-mail: info@auditor.sk.ca

AUDITOR'S REPORT

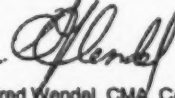
To the Members of the Legislative Assembly of Saskatchewan

I have audited the statement of financial position of the Office of the Information and Privacy Commissioner as at March 31, 2009 and the statements of operations and accumulated surplus, change in net assets, and cash flows for the year then ended. The Office is responsible for preparing these financial statements. My responsibility is to express an opinion on these financial statements based on my audit.

I conducted my audit in accordance with Canadian generally accepted auditing standards. Those standards require that I plan and perform an audit to obtain reasonable assurance whether the financial statements are free of material misstatement. An audit includes examining, on a test basis, evidence supporting the amounts and disclosures in the financial statements. An audit also includes assessing the accounting principles used and significant estimates made by management, as well as evaluating the overall financial statement presentation.

In my opinion, these financial statements present fairly, in all material respects, the financial position of the Office of the Information and Privacy Commissioner at March 31, 2009 and the results of its operations and its cash flows for the year then ended in accordance with Canadian generally accepted accounting principles.

Regina, Saskatchewan
May 29, 2009


Fred Wendel, CMA, CA
Provincial Auditor



2008 - 2009 ANNUAL REPORT

Saskatchewan
Information and Privacy
Commissioner



503 - 1801 Hamilton Street
Regina, Saskatchewan
S4P 4B4

Tel: (306) 787-8350
Fax: (306) 798-1603
Website: www.oipc.sk.ca

June 4, 2009

2008 - 2009 MANAGEMENT REPORT

The accompanying financial statements are the responsibility of management and have been approved in principle by the Office of the Information and Privacy Commissioner. The financial statements have been prepared in accordance with Canadian generally accepted accounting principles.

Management maintains appropriate systems of internal control, including policies and procedures which provide reasonable assurance that the Office's assets are safeguarded and that financial records are relevant and reliable.

The Provincial Auditor of Saskatchewan conducts an independent audit of the financial statements. His examination is conducted in accordance with Canadian generally accepted auditing standards and includes tests and other procedures which allow him to report on the fairness of the financial statements.

A stylized, handwritten signature in black ink, consisting of several loops and a long horizontal stroke.

R. Gary Dickson, Q.C.
Saskatchewan Information and
Privacy Commissioner

A handwritten signature in black ink, appearing to read 'Pam Scott' with a stylized flourish at the end.

Pam Scott
Manager of Administration



2008 - 2009 ANNUAL REPORT

Statement 1

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER STATEMENT OF FINANCIAL POSITION As at March 31

	2009	2008
Financial assets		
Due from the General Revenue Fund	\$ 79,815	\$ 35,252
Liabilities		
Accounts payable	71,055	27,520
Accrued employee costs	8,760	7,732
	<u>79,815</u>	<u>35,252</u>
Net assets	<u>---</u>	<u>---</u>
Non-financial assets		
Tangible capital assets (Note 3)	72,139	64,339
Prepaid expenses	8,329	5,253
	<u>80,468</u>	<u>69,592</u>
Accumulated surplus	<u>\$ 80,468</u>	<u>\$ 69,592</u>

(See accompanying notes to the financial statements)



Statement 2

**OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER
STATEMENT OF OPERATIONS AND ACCUMULATED SURPLUS
For the Year Ended March 31**

	2009		2008
	Budget	Actual	Actual
	(Note 4)		
Revenues			
General Revenue Fund - Appropriation	\$822,000	\$807,750	\$673,793
Registration Fee Revenue	—	7,700	—
Total Revenue		<u>815,450</u>	<u>673,793</u>
Expenses			
Salaries and other employment expenses	\$599,000	\$550,015	\$457,835
Administration and operating expenses	70,300	58,582	52,805
Rental of space and equipment	87,500	88,079	80,820
Travel	42,400	37,120	26,713
Advertising and promotion	19,300	26,691	17,048
Amortization	—	40,794	41,257
Contractual and legal services	3,500	3,293	1,406
Total Expenses	822,000	804,574	677,884
Annual surplus (deficit)	<u>\$ —</u>	10,876	(4,091)
Accumulated surplus, beginning of year		<u>69,592</u>	<u>73,683</u>
Accumulated surplus, end of year		<u>\$80,468</u>	<u>\$65,592</u>

(See accompanying notes to the financial statements)



2008 - 2009 ANNUAL REPORT

Statement 3

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER STATEMENT OF CHANGE IN NET ASSETS For the year ended March 31

	2009	2008
Annual surplus (deficit)	\$ 10,876	\$ (4,091)
Acquisition of tangible capital assets	\$ (48,594)	\$ (37,989)
Amortization of tangible capital assets	40,794	41,257
	(7,800)	3,268
(Increase) decrease in prepaid expense	(3,076)	823
	(10,876)	4,091
Decrease (Increase) in net assets	—	—
Net assets, beginning of year	—	—
Net assets, end of year	\$ —	\$ —

(See accompanying notes to the financial statements)



Statement 4

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER
STATEMENT OF CASH FLOWS
For the year ended March 31

	2009	2008
Cash flows from (used in) operating activities:		
General Revenue Fund appropriation received	\$ 770,887	\$ 664,333
Salaries paid	(548,987)	(468,234)
Supplies and other expenses paid	(173,306)	(158,110)
	<u>(722,293)</u>	<u>(626,344)</u>
Cash provided from operating activities	<u>48,594</u>	<u>37,989</u>
Cash flows from (used in) investing activities:		
Purchase of tangible capital assets	<u>(48,594)</u>	<u>(37,989)</u>
Cash (used in) investing activities	<u>(48,594)</u>	<u>(37,989)</u>
Increase (decrease) in cash and cash equivalents	---	---
Cash and cash equivalents, beginning of year	<u>---</u>	<u>---</u>
Cash and cash equivalents, end of year	\$ ---	\$ ---

(See accompanying notes to the financial statements)



**OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER
NOTES TO THE FINANCIAL STATEMENTS
MARCH 31, 2009**

1. Authority and description of operations

The Freedom of Information and Protection of Privacy Act (Act) states that the Lieutenant Governor in Council, on the recommendation of the Assembly, shall appoint an Information and Privacy Commissioner. The Commissioner is an officer of the Legislative Assembly and is appointed by resolution. The mandate of the Office of the Information and Privacy Commissioner (Office) is to review Government decisions under the Act to ensure the protection of the public's right to access records held or controlled by the Government and to ensure that personal information is only collected, used and disclosed according to the manner and purposes set out in the Act.

2. Summary of accounting policies

The Office uses Canadian generally accepted accounting principles to prepare its financial statements. The following accounting policies are considered to be significant.

a) Revenue

The Office receives an appropriation from the Legislative Assembly to carry out its work. General Revenue Fund appropriations are included in revenue when amounts are spent or committed. The Office's expenditures are limited to the amount appropriated to it by the Legislative Assembly.

b) Tangible capital assets

Tangible capital assets are reported at cost less accumulated amortization. Tangible capital assets are amortized on a straight-line basis over a life of three to five years. All tangible capital assets of \$50.00 or more have been capitalized.



3. Tangible capital assets

	2009				2008
	Hardware & Software	Furniture	Leasehold Improvements	Total	Total
Opening costs of tangible capital assets	\$54,422	\$96,821	\$43,852	\$195,095	\$157,105
Additions during year	18,003	30,590	—	48,593	37,989
Disposals during year	—	—	—	—	—
Closing costs of tangible capital assets	72,425	127,411	43,852	243,688	195,094
Opening accumulated amortization	44,916	65,399	20,440	130,755	89,498
Annual amortization	9,488	19,600	11,706	40,794	41,257
Closing accumulated amortization	54,404	84,999	32,146	171,549	130,755
Net book value of tangible capital assets	\$18,021	\$42,412	\$11,706	\$72,139	\$64,339

4. Budget

These amounts represent funds appropriated by the Board of Internal Economy to enable the Office to carry out its duties under *The Freedom of Information and Protection of Privacy Act*.

5. Costs borne by other agencies

The Office has not been charged with certain administrative costs. These costs are borne by the Legislative Assembly. No provision for these costs is reflected in these financial statements.



6. Lapsing of appropriation

The Office follows *The Financial Administration Act, 1993* with regards to its spending. If the Office spends less than its appropriation by March 31, it must return the difference to the General Revenue Fund.

7. Financial Instruments

The Office's financial instruments include Due from the General Revenue Fund, Accounts payable and Accrued employee payables. The carrying amount of these instruments approximates fair value due to their immediate or short-term maturity. These instruments have no significant interest rate and credit risk.



Appendices



Appendix I - Definitions

The following is a list of definitions of terms or abbreviations used in the course of this document or referenced in documents accessible from the website: www.oipc.sk.ca.

Additional definitions are found in the three provincial statutes: *The Freedom of Information and Protection of Privacy Act* (FOIP), *The Local Authority Freedom of Information and Protection of Privacy Act* (LA FOIP) and *The Health Information Protection Act* (HIPA).

Applicant refers to an individual who has made an access request to a government institution, local authority, or health information trustee.

Access is the right of an individual (or his or her lawfully authorized representative) to view or obtain copies of records in the possession or control of a government institution, local authority or trustee including his/or her personal information/personal health information.

Commissioner refers to the Saskatchewan Information and Privacy Commissioner.

Complainant refers to an aggrieved individual who makes a formal complaint to the Commissioner to investigate an alleged "unreasonable invasion of privacy" by that public body pursuant to sections 33 of FOIP, 32 of LA FOIP, or 52 of HIPA.

Complaint is written concern that there has been a breach of privacy by a government institution, local authority or trustee.

Confidentiality is the protection of personal information and personal health information once obtained against improper or unauthorized use or disclosure. This is just one aspect of privacy and is not synonymous with 'privacy'.

Control is a term used to indicate that the records in question are not in the physical possession of the public body or trustee, yet still within the influence of that body via another mechanism (e.g. contracted service).

Custody is the physical possession of a record by a public body or trustee.



Appendix I - Definitions

Detailed Advice and Commentary refers to requests for evaluative, general, non-binding advice that take in excess of one hour of research, most of these would involve in excess of 4 hours research.

Disclosure is sharing of personal information with a separate entity, not a division or branch of the public body or trustee in possession or control of that record/information.

Duty to Assist means responding openly, accurately and completely to an individual requesting access to records in the possession or control of a government institution or local authority or to personal health information in the custody or control of a health information trustee.

Exclusions are prescribed records and organizations that are not subject to FOIP, LA FOIP or HIPA.

Exemptions are sections of the relevant statutes referenced to justify the denial of access to records by the individual either for mandatory or discretionary reasons.

FOIP refers to *The Freedom of Information and Protection of Privacy Act* that came into force in 1992.

FOIP Coordinator refers to an individual designated pursuant to section 60 of FOIP for managing access and privacy issues in any public body with this title.

FOIP Regime means the statute, regulations, policies, practices and procedures followed in the operation of the statutes.

Government Institution refers to those public bodies prescribed in FOIP and the FOIP Regulations and includes more than 70 provincial government departments, agencies, and Crown corporations.

Head of a public body is the individual accountable by law for making the final decision on access requests, but may delegate these powers to someone else in the organization. This is typically the Minister of a department and the CEO of a local authority or Crown corporation.



Appendix I - Definitions

HIPA refers to *The Health Information Protection Act* that came into force in 2003.

Identity Theft occurs when one person uses another's personal information without his/her knowledge or consent to commit a crime such as fraud or theft.

LA FOIP refers to *The Local Authority Freedom of Information and Protection of Privacy Act* that came into force in 1993.

Local Authorities means local government including library boards, municipalities, regional colleges, schools, universities, and Regional Health Authorities as prescribed by LA FOIP and the LA FOIP Regulations.

Mediation is the process of facilitating discussion between the parties involved in a review or investigation by the OIPC with the goal of negotiating a mutually acceptable resolution to the dispute without the issuance of a formal report.

OIPC is an abbreviation for the Office of the Saskatchewan Information and Privacy Commissioner.

Personal Information is "recorded information about an identifiable individual" and includes details such as your name, address, phone number, SIN, race, driver's license number, health card number, credit ratings, and opinions of another person about you.

Personal Health Information includes information about your physical or mental health and/or information gathered in the course of providing health services for you.

PIA is an abbreviation for a Privacy Impact Assessment. A PIA is a diagnostic tool designed to help organizations assess their compliance with the privacy requirements of Saskatchewan legislation.

Privacy, in terms of 'information privacy,' means the right of the individual to determine when, how and to what extent he/she will share information about him/herself with others. Privacy captures both security and confidentiality of personal information/personal health information.

Privacy Breach happens when there is an unauthorized collection, use or disclosure of personal information/personal health information regardless of whether the



Appendix I - Definitions

Public Bodies are organizations in the public sector including government institutions and local authorities.

Record is information in any form or format and includes such items as documents, maps, books, post-it notes, handwritten notes, phone messages, photographs, and tape recordings.

Report is a document prepared by the Saskatchewan Information and Privacy Commissioner that issues recommendations to a public body for changes and/or actions in response to the findings of a formal access review or breach of privacy complaint.

Research is the systematic investigation designed to develop or establish principles, facts or generalizable knowledge.

Secondary Purpose refers to the use or disclosure of personal information/personal health information for a purpose other than that for which it was originally collected.

Security refers to steps taken to protect personal information or personal health information from unauthorized disclosure.

Summary advice refers to requests for information received from public bodies or the public that can be responded to with less than one hour of research

Surrogate refers to someone other than the individual but who is exercising rights or powers under section 59 of FOIP, sections 49 or 56 of HIPA on behalf of the individual.

Third Party is a person other than the applicant or a public body.

Trustees as defined within section 2(t) of HIPA are individuals and corporations who are part of Saskatchewan's health system in custody or control of personal health information and any government institution as defined by FOIP.

Use indicates the internal utilization of personal information by a public body and includes sharing of the personal information in such a way that it remains under the control of that public body.



Appendix II - Sample List of Presentations

April 1, 2008 to March 31, 2009

- The Association for Records and Information Management Professionals (ARMA)
- Brown Bag Luncheon – "Severing Made Easy"
- Canadian Cancer Society
- Canadian Association of Law Libraries
- Canadian Bar Association Alberta Law Conference 2009
- Canadian Bar Association Access and Privacy Section Meeting
- Canadian Council of Archives
- Career and Employment Services Annual Forum
- College of Psychologists – Professional Practice and Ethics Committee
- Consumers' Association of Canada
- Cypress Regional Health Authority
- Federal/Provincial/Territorial FOIP Managers
- Health Quality Council
- Lakeland Library Region
- Legislative Interns Orientation
- Lorman Education Services
- Ministry of Advanced Education, Employment and Labour
- Network of Intra-provincial Regulatory Organizations (NIRO)
- Planned Parenthood
- Prairie Health Information Privacy Conference
- Regina Community Clinic
- Saskatchewan College of Psychologists – Annual General Meeting
- Saskatchewan Registered Nurses' Association Interdisciplinary Conference
- Saskatchewan Watershed Authority
- South Saskatchewan Independent Living Centre
- University of Regina – Investigative Journalism Class
- University of Regina – Political Science Class
- University of Regina – Politics of Media Class
- University of Saskatchewan – Law Faculty



Appendix III - List of Bodies Subject to OIPC Oversight

Government Institutions (90+)

Local Authorities

Libraries (589)

Municipalities:

13 cities and 455 other **urban municipalities** including:

147 towns

268 villages

40 resort villages

Southern Saskatchewan has 296 **rural municipalities**

The rural municipalities include 172 organized hamlets.

In Northern Saskatchewan there are:

2 towns

11 northern villages

12 northern hamlets

10 northern settlements

Regional Colleges (8)

Regional Health Authorities (13)

School Divisions (29)

SIAST (4 campuses)

Universities (2)

Health Information Trustees

(Others may be added through regulations)

Ambulance Operators

Community Clinics

Government Institutions

20 Ministries

77 Crown Corporations and Agencies



Appendix III - List of Bodies Subject to OIPC Oversight

Health Profession Regulatory Bodies

- Chiropractors Association of Saskatchewan
- College of Dental Surgeons of Saskatchewan
- College of Physicians and Surgeons of Saskatchewan
- Dental Technicians Association of Saskatchewan
- Denturist Society of Saskatchewan
- Registered Psychiatric Nurses Association of Saskatchewan
- Saskatchewan Association of Chiropodists
- Saskatchewan Association of Licensed Practical Nurses
- Saskatchewan Association of Medical Radiation Technologists
- Saskatchewan Association of Naturopathic Practitioners
- Saskatchewan Association of Optometrists
- Saskatchewan Association of Social Workers
- Saskatchewan Association of Speech/Language Pathologists and Audiologists
- Saskatchewan College of Midwives
- Saskatchewan College of Pharmacists
- Saskatchewan College of Physical Therapists
- Saskatchewan College of Podiatrists
- Saskatchewan College of Psychologists
- Saskatchewan Dental Assistants Association
- Saskatchewan Dental Hygienists Association
- Saskatchewan Dental Therapists Association
- Saskatchewan Dieticians Association
- Saskatchewan Ophthalmic Dispensers Association
- Saskatchewan Registered Nurses' Association
- Saskatchewan Society for Medical Laboratory Technologists
- Saskatchewan Society of Occupational Therapists



Appendix III - List of Bodies Subject to OIPC Oversight

Laboratories
Mental Health Facilities
Personal Care Homes
Pharmacies
Regional Health Authorities and Affiliates
 13 health authorities
Regulated Health Professions
 1500 physicians and surgeons
 9200 registered nurses
Saskatchewan Cancer Agency
Special Care Homes



Endnotes

- 1 Colin J. Bennett, *The Privacy Commissioner of Canada: Multiple Roles, Diverse Expectations and Structural Dilemmas*, *Canadian Public Administration* Vol 46, No. 2.
- 2 See *Nautical Data International Inc. v. Canada (Minister of Fisheries and Oceans)*, 2005 FC 407 at para.8; *Canada (Attorney General) v. Canada (Information Commissioner)*, [2004] 4 F.C.R. 181 at para. 20, 255 F.T.R. 56, 15 Admin. L.R. (4th) 58, 32, C.P.R. (4th) 464, 117 C.P.R. (2d) 85, 2004 FC 431, rev'd (2005), 253 D.R.R. (4th) 590, 335 N.R. 8, 40 C.P.R. (4th) 97, 2005 FCA 199, leave to appeal to S.C.C. requested; *Canada (Attorney General) v. Canada (Information Commissioner)*, [2002] 3 F.C. 630 at para. 20, 216 F.T.R. 247, 41 Admin. L.R. (3d) 237, 2002 FCT 128, 2430901; *Canada Inc. v. Canada (Minister of Industry)*, [2002] 1 F.C. 421 at para. 102, (2001), 282 N.R. 284, 45 Admin L.R. (3d) 182, (2001) 14 C.P.R. (4th) 449, 2001 FCA 254, leave to appeal to S.C.C. refused, [2001] S.C.C.A. No 537 (Q.L.); *Lavigne v. Canada (Office of the Commissioner of Official Languages)*, [2002] 2 S.C.R. 773, (2002) SCC 53 at para 25; *R. v. Dymont*, [1988] 2 S.C.R. 417; *R. v. Mills*, [1999] 3 S.C.R. 668; *Dagg v. Canada (Minister of Finance)*, [1997] 2 S.C.R. 402; *R. v. Plant*, [1993] 3 S.C.R. 281; *R. v. Duarte*, [1990] 1 S.C.R. 30; *R. v. Edward*, [1996] 1 S.C.R. 128; *Canada (Information Commissioner) v. Canada (Commissioner of the Royal Canadian Mounted Police)*, [2003] 1 S.C.R. 66, 2003 SCC 8
- 3 2004 - 2005 Annual Report of the Saskatchewan Information and Privacy Commissioner (page 10). Available online at: <http://www.oipc.sk.ca/Reports/AnnualReport04-05.pdf>
- 4 Section 68 of *The Freedom of Information and Protection of Privacy Act*, S.S. 1990-91, c. F-22.01. Available online at: <http://www.qp.gov.sk.ca/documents/English/Statutes/Statutes/F22-01.pdf>
- 5 Available online at: <http://www2.parl.gc.ca/CommitteeBusiness/CommitteeHome.aspx?Cmte=ETHI&Language=E&Mode=I&Parl=40&Ses=2>
- 6 Supra Note 3
- 7 *The Privacy Act*, S.S. 2004 c.L-16.1. Available online at: <http://www.qp.gov.sk.ca/documents/English/Statutes/Statutes/P24.pdf>
- 8 *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c.5 as amended. Available online at: <http://www2.parl.gc.ca/HousePublications/Publication.aspx?pub=bill&doc=C-6&parl=36&ses=2&language=E>



Endnotes

- 9 *The Workers' Compensation Act, 1979*, S.S. 1979, c. W-17.1. Available online at: <http://www.qp.gov.sk.ca/documents/English/Statutes/Statutes/W17-1.pdf>
- 10 Committee of Review, 2006 Report p. 224
- 11 Report of the Honourable E.M. Culliton, Former Chief Justice of Saskatchewan, *On the Matter of Freedom of Information and Protection of Privacy in the Province of Saskatchewan* (1982).
- 12 *Access to Information Act*, R.S. 1985, c. A-1. Available online at: <http://laws.justice.gc.ca/en/a-1/text.html>
- 13 *Privacy Act*, R.S. 1985, c. P-21. Available online at: <http://laws.justice.gc.ca/en/P-21/93298.html>
- 14 Available online at: http://www.sgi.sk.ca/news_releases/2009/mar_23_2009.html
- 15 Available online at: <http://www.lawsociety.sk.ca/>
- 16 Available online at: <http://www.oipc.sk.ca/Resources/PIAIntro-December2005.pdf>





2008 – 2009 ANNUAL REPORT ERRATUM

of the SASKATCHEWAN INFORMATION AND PRIVACY COMMISSIONER

Page 3, second paragraph

Change the sentence from "Four years ago we had only two privacy investigations." to

"Six years ago we had only two privacy investigations."

Page 13, first paragraph

Change the sentence from "I should note that those employees who work for an enterprise that qualifies as a 'federal work, undertaking or business' such as airlines, banking, telecommunications and interprovincial trucking are covered by *Personal Information Protection of Electronics Document Act* (PIPEDA)." to

"I should note that those employees who work for an enterprise that qualifies as a 'federal work, undertaking or business' such as airlines, banking, telecommunications and interprovincial trucking are covered by the *Personal Information Protection and Electronic Documents Act* (PIPEDA)."

Page 29, third paragraph

Change the sentence from "Presumably the purpose of section 11 of HIPA was to ensure that widespread demands for production and collection of copies of health services cards would undermine confidence of patients in the security of their personal health information in an EHR world." to

"Presumably the purpose of section 11 of HIPA was to avoid widespread demands for production and collection of copies of health services cards that would undermine the confidence of patients in the security of their personal health information in an EHR world."